A Graphic Representation of States for Quantum Copying Machines

Sara Felloni[1,e] and Giuliano Strini[2]

[1] Dipartimento di Informatica, Sistemistica e Comunicazione
Università degli Studi di Milano – Bicocca
Via Bicocca degli Arcimboldi 8, 20126 Milano, Italy

[2] Dipartimento di Fisica
Università degli Studi di Milano
Via Celoria 16, 20133 Milano, Italy

[e] e-mail: sara.felloni@disco.unimib.it

Abstract

The aim of this paper is to introduce a new graphic representation of quantum states by means of a specific application: the analysis of two models of quantum copying machines.

The graphic representation by diagrams of states offers a clear and detailed visualization of quantum information's flow during the unitary evolution of not too complex systems. The diagrams of states are exponentially more complex in respect to the standard representation and this clearly illustrates the discrepancy of computational power between quantum and classical systems.

After a brief introductive exposure of the general theory, we present a constructive procedure to illustrate the new representation by means of concrete examples. Elementary diagrams of states for single-qubit and two-qubit systems and a simple scheme to represent entangled states are presented. Quantum copying machines as imperfect cloners of quantum states are introduced and the quantum copying machines of Griffiths and Niu and of Bužek and Hillery are analyzed, determining quantum circuits of easier interpretation.

The method has indeed shown itself to be extremely successful for the representation of the involved quantum operations and it has allowed to point out the characteristic aspects of the quantum computations examined.

1 Introduction

We explore the possibility of a not necessarily new representation but certainly of rare use in literature: the graphic representation of states, in opposi-

tion to the analytical representation and to Feynman's diagrams, considered still standard today.

The graphic representation of states is exponentially more complex in respect to the standard representation, but this characteristic is considered a merit rather than a flaw, since it makes it possible to obtain a clear visualization of the most minute details that do not appear so evident in too concise representations and thus are not always easily comprehensible. The exponential increase of dimension of the diagram of states in respect to the number of qubits that constitute the system clearly illustrates the discrepancy of computational power between quantum and classical systems. At the same time, the use of such graphic representation offers a clear visualization of quantum information's flow and of the key-steps of computation during the evolution of the system.

After a brief introductive exposure of the general theory, we present a constructive procedure to illustrate the new representation by means of concrete examples. Our choice is to explore two models of quantum copying machines by means of analytical representation, standard quantum circuits and diagrams of state, to detect the indicative details of systems and processes considered.

The paper is organized as follows. In section 2 the new graphical method to analyze quantum information's flow, the diagrams of states, is introduced: elementary diagrams of states for single-qubit and two-qubit systems and a simple scheme to represent entangled states are illustrated. Section 3 intruduces quantum copying machines as imperfect cloners of quantum states. The quantum copying machine of Griffiths and Niu and the quantum copying machine of Bužek and Hillery are analyzed respectively in sections 3.1 and 3.2: they allow to present a first example of graphic representation by diagrams of states, very useful in determining quantum circuits of easier interpretation. The analysis of the quantum copying machine of Bužek and Hillery is discussed for both symmetrical and asymmetrical behaviors, each case related to the cryptographic protocol used by the two communicating parties: in the symmetrical case a *six-state* protocol requires isotropic cloning of the information transmitted, while in the asymmetrical case the isotropy conditions may be relaxed when a *four-state* protocol is used. Finally, in section 4 our conclusions and some possible directions for future research from the present work are presented, while further details are left in appendixes.

In all the following quantum circuits and diagrams of states, any sequence of logic gates must be read from the left (input) to the right (output); from top to bottom, qubits run from the least significant (LSB) to the most significant (MSB).

2 The graphic representation of states

2.1 Elementary Diagrams of States

In many situations it can be useful to perform different representations of the issue aimed to study, in order to compare the different typologies of analysis.

To this purpose we introduce a new graphic method, the diagrams of states, directly derived from the standard Feynman representation of quantum circuit. In our opinion, this new graphic representation of states is potentially useful for a clear and intuitive visualization of quantum information's flow during the unitary evolution of not too complex systems.

First, elementary diagrams of states for a system constituted by a single qubit (correspondingly, by two states), are shown in figure 1. They represent the elementary operations listed and described below:

1. *not* gate;
2. unitary matrix.

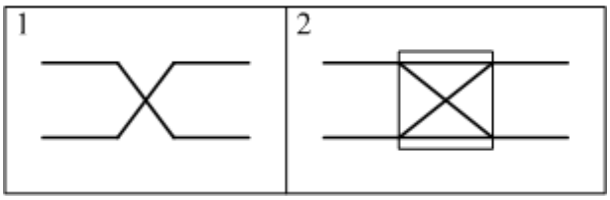

Figure 1: Single-qubit elementary diagrams of states.

The diagram of states of the *not* gate clearly illustrates that the two states are switched. The unitary matrix is represented by four intersecting lines, each one labeled with the corresponding entry of the matrix.[1]

Then, elementary diagrams of states for a system constituted by two qubit (whose corresponding state space is described by four states) are shown in figures 2-6. They comprehend both the previously illustrated single-qubit gates, now set into the state space of two qubits, and the two-qubit gates, all of them listed and described below:

[1]It will result clear from the following quantum circuits that this representation is particularly useful to show constructive and destructive interferences in information's flow.

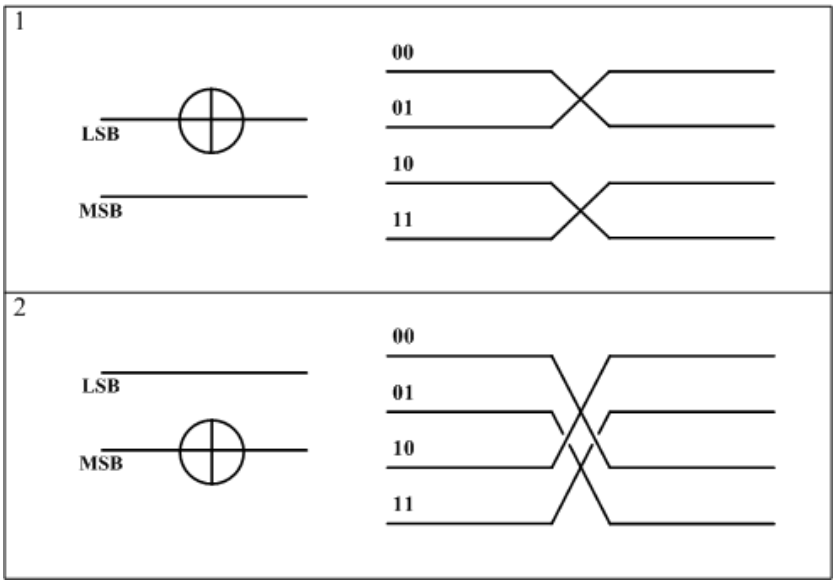

Figure 2: Diagrams of states for two-qubits systems: *not* gates on the least significant bit and on the most significant bit.

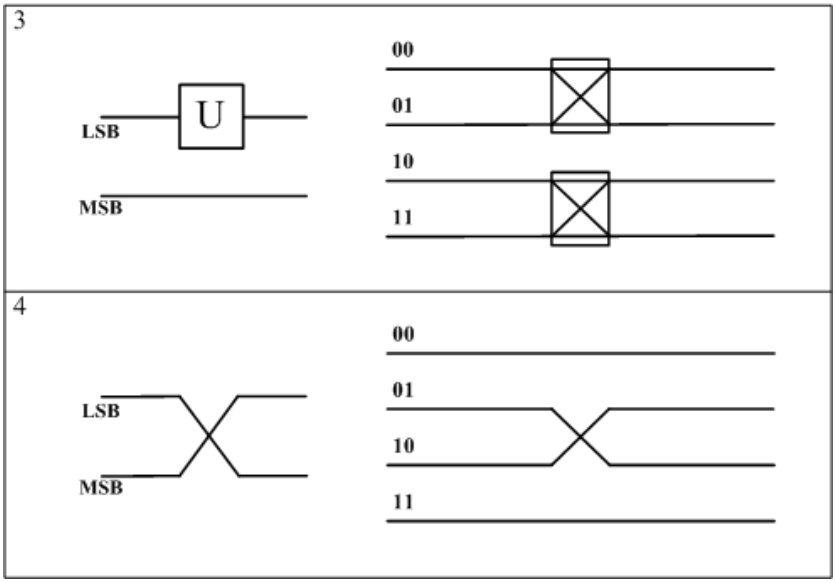

Figure 3: Diagrams of states for two-qubits systems: unitary matrix on the least significant bit and *swap* gate.

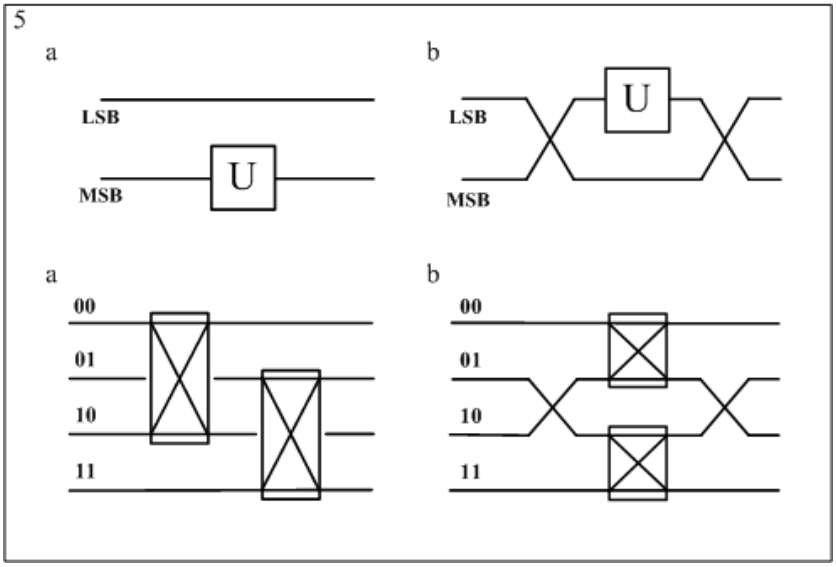

Figure 4: Diagrams of states for two-qubits systems: unitary matrix on the most significant bit; the more widely used representation (a) and an alternative one (b).

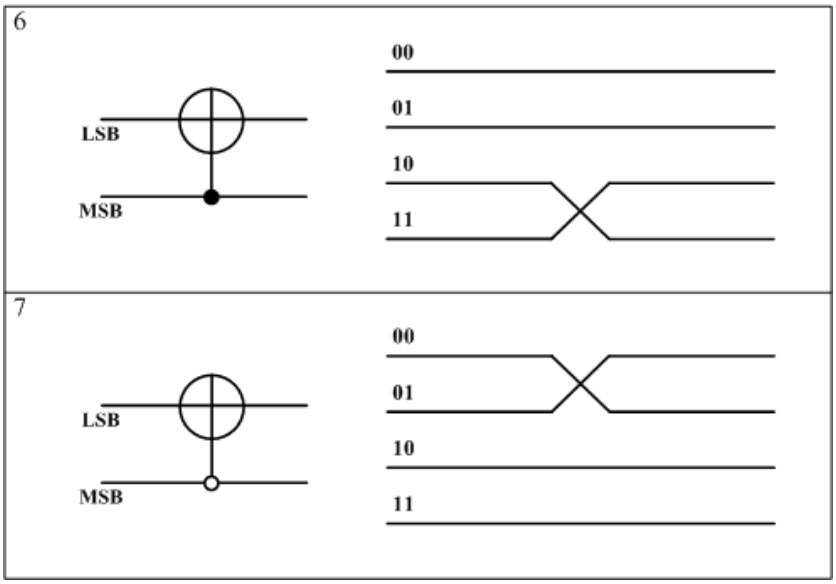

Figure 5: Diagrams of states for two-qubits systems: *c-not* and $\overline{c-not}$ gates.

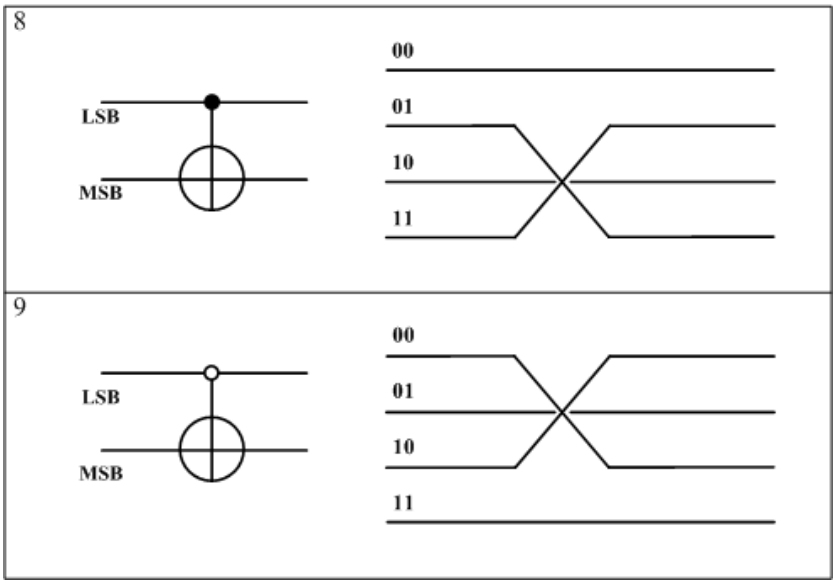

Figure 6: Diagrams of states for two-qubits systems: $c-not-R$ and $\overline{c-not-R}$ gate.

1. *not* gate on the least significant bit

$$V = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix};$$

2. *not* gate on the most significant bit

$$V = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix};$$

3. unitary matrix on the least significant bit

$$V = \begin{bmatrix} \mathbf{U} & \mathbf{0} \\ \mathbf{0} & \mathbf{U} \end{bmatrix};$$

4. *swap* gate

$$swap = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix};$$

5. unitary matrix on the most significant bit

$$V = \mathbf{U} \otimes \mathbb{I};$$

6. *c-not* gate

$$c - not = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix};$$

7. $\overline{c - not}$ gate

$$\overline{c - not} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix};$$

8. $c - not - R$ gate

$$c - not - R = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix};$$

9. $\overline{c - not - R}$ gate

$$\overline{c - not - R} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

The *not* gate on the least significant bit is represented by the switches of the couples of states $\{00, 01\}$ and $\{10, 11\}$, while the not gate on the most significant bit switches of the couples of states $\{00, 10\}$ and $\{01, 11\}$. Notice that the lines corresponding to switches of states do intersect while states that do not switch correspond to overlapping (not intersecting) lines.

The state diagram for a unitary matrix on the least significant bit is obtained by applying the single-qubit scheme for the unitary matrix presented above (see figure 1, diagram 2) to the couples of states $\{00, 01\}$ and $\{10, 11\}$.

The *swap* gate switches the states 01 and 10, leaving the states 00 and 11 unchanged.

The diagram of states for a unitary matrix on the most significant bit is obtained by applying twice the single-qubit scheme for the unitary matrix to the couples of states $\{00, 10\}$ and $\{01, 11\}$. As before, notice that the lines of the states to which the unitary matrix is applied do intersect while the other lines are overlapping and not intersecting. In addition to this

more widely used representation, labeled with (a) in figure 4, an alternative representation, labeled with (b) and usually less convenient than the first one, is also offered. In this case, the unitary matrix on the most significant bit can be obtained by applying two *swap* gates and the unitary matrix on the least significant bit (whose scheme is presented in figure 3, diagram 3).

The $c-not$ gate switches the states that correspond to MSB$=1$, that is the couple $\{10, 11\}$. The $\overline{c-not}$ gate does the same operation for MSB$=0$ and thus the states $\{00, 01\}$ are switched. The $c-not-R$ and $\overline{c-not-R}$ gates do similar operations with the control now set on the least significant bit (instead of the most significant bit): the first gate switches the couples of states $\{01, 11\}$ while the second gate switches the couple of states $\{00, 10\}$. As before, states that do not switch correspond to overlapping (not intersecting) lines.

Generalization to system of a greater number of qubits can be immediately drawn from the present procedure.

2.1.1 Representation of the *Entanglement* by means of the Diagrams of States

The diagrams of states also allow to represent *entanglement* by means of a very useful and simple scheme, as shown in figure 7.

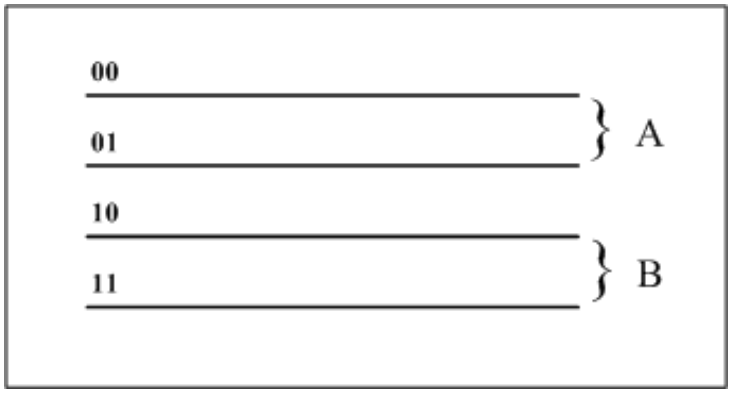

Figure 7: Diagram of states representing the *entanglement* of two states.

In this diagram, the couples of lines, labeled with A and B, correspond to the state of the least significant bit respectively associated to the value $|0\rangle$ and to the value $|1\rangle$ of the most significant bit: A labels the couple of states $\{00, 01\}$ and B labels the couple of states $\{10, 11\}$. It can be easily seen that *entanglement* takes place if the couples of states A and B differ for more than a simple factor: in this case the overall state cannot be factorized in two single-qubit states.

This representation of *entanglement* can be immediately generalized to k qubits, in which case the diagram will be composed by ordered sub-diagrams of 2^k elements. A further generalization can be made considering a n-level system, known as qunit. So if a system of k qunits is instead considered, its diagram will be composed by ordered sub-diagrams of n^k elements.

The exponential increase of dimension of the diagram of states in respect to the number of qubits (or qunits) that constitute the system clearly illustrates the discrepancy of computational power between quantum and classical systems; at the same time, the use of such graphic representation offers a clear visualization of the information's flow in quantum space and of the key-steps of the whole procedure.

3 Quantum Copying Machines

The *No Cloning Theorem*[2] affirms the impossibility to realize a machine able to clone the state of a generic qubit, that is the impossibility, given in input a qubit in a generic state, to get two or more qubits in an identical state as output; [4],[5].

Thus the system in figure 8, where **U** is an unitary matrix that represents the action performed on the input and the ancillary qubits, in order to get two exact copies of the first one, cannot be realized.

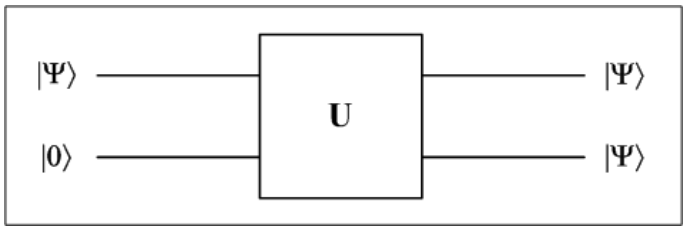

Figure 8: Schematic drawing of an hypotethical perfect quantum copying machine.

This impossibility is precisely what constitutes the basis of all quantum cryptographic systems.

However a generalization of such an operation, that results being of great interest in several fields of quantum computation and information processing, can be considered. If the request of perfect copies is given up, it is possible to restrict the search to copies as imperfect clones, since such a

[2]The *No Cloning Theorem* (due to Dieks, Wootters and Zurek; [4],[5]), well known and of great importance since it summarizes many aspects of Quantum Mechanics in an extremely simple synthesis, has been exposed in ref.[12], where more possible demonstrations have been presented, each of them related to different aspects of quantum theory.

procedure does not contradict the *No Cloning Theorem*, which sets limitations only on perfect copies.

Thus the former scheme is replaced by the one in figure 9, where $\mathbf{U}$ is still an unitary matrix that represents the action of "copying", but the states $|a_i\rangle$, for $i = 0, 1$, are not required anymore to be exactly the state $|\Psi\rangle$. In such a case it is possible to obtain states $|a_i\rangle$ not identical to the state to copy, $|\Psi\rangle$, but resembling it according to different criteria.

The use of one or more ancillary qubits, that will be discarded at the end of the transformation given by the unitary matrix $\mathbf{U}$, is a standard procedure in many situations in which more general transformations in respect to simple unitary transformations are desirable, as the one shown in figure 9. For further details refer to [1],[2],[3].

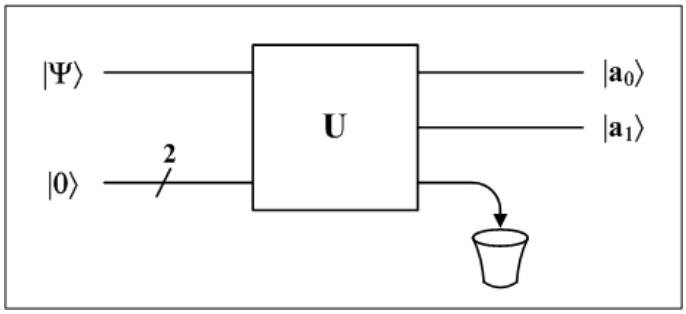

Figure 9: Schematic drawing of a general imperfect quantum copying machine.

In quantum cryptography such a procedure can be applied by an eavesdropper (traditionally called Eve) who aims to create a copy of the qubit transmitted by the authorized sender to the authorized receiver (traditionally called Alice and Bob) in cryptographic protocols.[3] After having intercepted the transmitted state, $|\Psi\rangle$, Eve sends an imperfect copy, $|a_0\rangle$, to Bob and she keeps for herself a second imperfect copy, $|a_1\rangle$, on which subsequently she will perform opportune measurements. In such operation Eve has fundamentally two goals to achieve: on the one hand she wishes to make her intrusion as unknown as possible to the two communicating parties, and on the other hand she wishes to find out as much information as possible on the state originally transmitted by Alice, $|\Psi\rangle$, by measuring her imperfect copy $|a_1\rangle$.

So the analysis of the overall system mainly consists in determining the unitary matrix $\mathbf{U}$ that optimizes the system in respect to the security of communication (Bob) or to the best possible intrusion (Eve).[4]

[3]Here and in the following sections, the two authorized communicating parties, sender and receiver, and the eavesdropper will be indicated as Alice, Bob and Eve, respectively.

[4]The specific kind of attack to quantum cryptographic systems by means of intrusion

3.1 The Griffiths-Niu Copying Machine

The original version of the Griffiths-Niu copying machine, [6],[7], in figure 10, shows the drawback not to possess the identity: if the perturbation gates (the control-$\frac{\theta_0}{2}$ and control-$\frac{\theta_1}{2}$ gates) are absent, the outcomes of Bob and Eve are exchanged by the circuit.

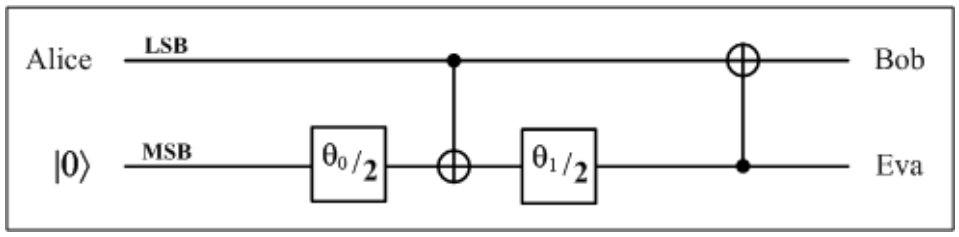

Figure 10: Schematic drawing of the original Griffiths-Niu quantum copying machine.

This situation in which, with no perturbation, Bob's and Eve's outcomes are switched is somehow counterintuitive but this drawback can be easily solved by adding at the end of the circuit a *swap* gate.

The *swap* gate can be synthetized by three *c-not* gates as shown in figure 11.

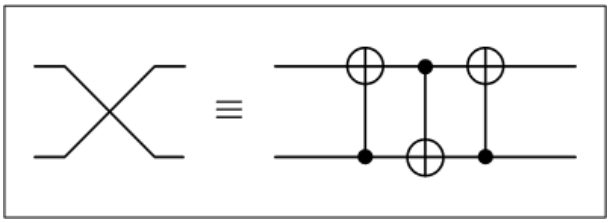

Figure 11: Quantum circuit implementing the synthesis of the *swap* gate by means of three *c-not* gates.

Since $c\text{-}not^2 = \mathbf{I}$, the two identical adjacent *c-not* gates can be simplified, thus obtaining a modified quantum copying machine, whose quantum circuit is presented in figure 12.

Defining:

$$C_{0,1} = cos\,\frac{\theta_{0,1}}{2} \qquad S_{0,1} = sin\,\frac{\theta_{0,1}}{2} \tag{1}$$

with quantum copying machines has been partially examined in ref.[12], where the intrusion/perturbation rate has been studied on the basis of limitations imposed by Quantum Mechanics for quantum copying machines with general characteristics; the present work aims to complete and improve such study.

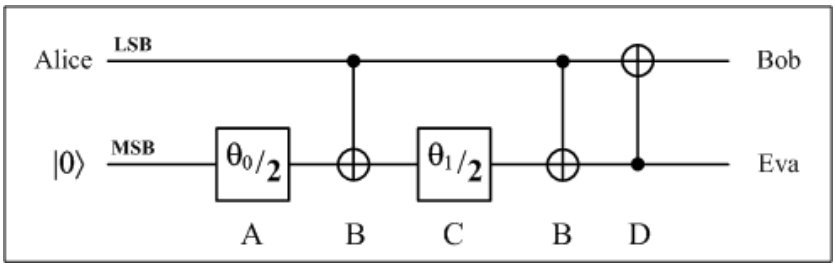

Figure 12: Schematic drawing of a modified Griffiths-Niu quantum copying machine by means of a *swap* gate.

the matrices of the quantum circuit in figure 12 can be expressed as follows:

$$A = \begin{bmatrix} C_0 & 0 & S_0 & 0 \\ 0 & C_0 & 0 & S_0 \\ -S_0 & 0 & C_0 & 0 \\ 0 & -S_0 & 0 & C_0 \end{bmatrix} \qquad B = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \tag{2}$$

$$C = \begin{bmatrix} C_1 & 0 & S_1 & 0 \\ 0 & C_1 & 0 & S_1 \\ -S_1 & 0 & C_1 & 0 \\ 0 & -S_1 & 0 & C_1 \end{bmatrix} \qquad D = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{3}$$

By multiplying matrices, the overall operation is given by:

$$D\,B\,C\,B\,A = \begin{bmatrix} C_\alpha & 0 & S_\alpha & 0 \\ 0 & C_\beta & 0 & S_\beta \\ 0 & -S_\beta & 0 & C_\beta \\ -S_\alpha & 0 & C_\alpha & 0 \end{bmatrix} \tag{4}$$

having defined:

$$C_{\alpha,\beta} = cos\,\alpha,\beta \qquad S_{\alpha,\beta} = sin\,\alpha,\beta \tag{5}$$

$$\alpha = \frac{\theta_0 + \theta_1}{2} \qquad \beta = \frac{\theta_0 - \theta_1}{2} \tag{6}$$

Defining $|\Psi_{in}\rangle$ as the initial state given by the state of Alice and the ancilla:

$$|\Psi_{in}\rangle = |0\rangle \otimes \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ b \\ 0 \\ 0 \end{bmatrix} \tag{7}$$

the output state can be easily calculated:

$$|\Psi_{out}\rangle = D\,B\,C\,B\,A\,|\Psi_{in}\rangle = \begin{bmatrix} C_\alpha\,a \\ C_\beta\,b \\ -S_\beta\,b \\ -S_\alpha\,a \end{bmatrix} \tag{8}$$

From this expression the density matrix of the final state can be drawn:

$$\rho = |\Psi_{out}\rangle\langle\Psi_{out}|$$

and subsequently Bob's density matrix ρ_{Bob}, by tracing the density matrix ρ over Eve's qubit, and Eve's density matrix ρ_{Eve}, by tracing the density matrix ρ over Bob's qubit:

$$\rho_{Bob} = Tr_{MSB}\,\{\rho\} \qquad\qquad \rho_{Eve} = Tr_{LSB}\,\{\rho\}$$

Finally, Bob and Eve's density matrices are expressed in the Bloch sphere representation, that provides an useful visualization of quantum states and of their transformations. The Bloch sphere can be embedded in a three-dimensional space of Cartesian coordinates: here and in the following sections, we call $\{X, Y, Z\}$ the Bloch sphere coordinates of the qubit sent from Alice to Bob before eavesdropping and $\{X_i, Y_i, Z_i\}$, for $i = B, E$, the Bloch sphere coordinates associated to Bob and Eve's density matrices ρ_{Bob}, ρ_{Eve} after eavesdropping.

Bob and Eve's density matrices are then represented in Bloch sphere coordinates, expressed as a function of the coordinates $\{X, Y, Z\}$ of the initial density matrix of Alice's pure state:

$$\begin{cases} X_B = [C_\alpha\,C_\beta + S_\alpha\,S_\beta]\,X \\ Y_B = [C_\alpha\,C_\beta - S_\alpha\,S_\beta]\,Y \\ Z_B = [C_\alpha^2 - C_\beta^2] + [C_\alpha^2 - S_\beta^2]\,Z \end{cases} \tag{9}$$

$$\begin{cases} X_E = -\,[C_\alpha\,S_\beta + S_\alpha\,C_\beta]\,X \\ Y_E = [-C_\alpha\,S_\beta + S_\alpha\,C_\beta]\,Y \\ Z_E = [C_\alpha^2 - S_\beta^2] + [C_\alpha^2 - C_\beta^2]\,Z \end{cases} \tag{10}$$

These expressions can be obviously simplified. Observe that in both cases there is a displacement of the Bloch sphere and this constitutes a strong limitation to the effective utility of such quantum copying machine. However, the simplicity of the Griffiths-Niu copying machine, given by the possibility to describe the system by means of only two qubits (and correspondingly by means of only four states), allows us to introduce in the simplest possible way the diagrams of states, shown in figure 13.

From the quantum circuit in figure 12, by means of the representations illustrated in section 2, the upper diagram of states in figure 13 can be immediately drawn. From left to right, the diagram starts with the initial state: information flows on the marked lines labeled with $\{a, b\}$, while thinner lines correspond to absence of information, since the initial state of the most significant bit is set to the value $|0\rangle$. Then operators from A to D are applied in sequence, represented by the corresponding schemes for two-qubit gates. At the right end of the diagram, the final states can be observed.

This diagram can be simplified in an equivalent one, illustrated in figure 13 (bottom), where information's flow can be easily followed.

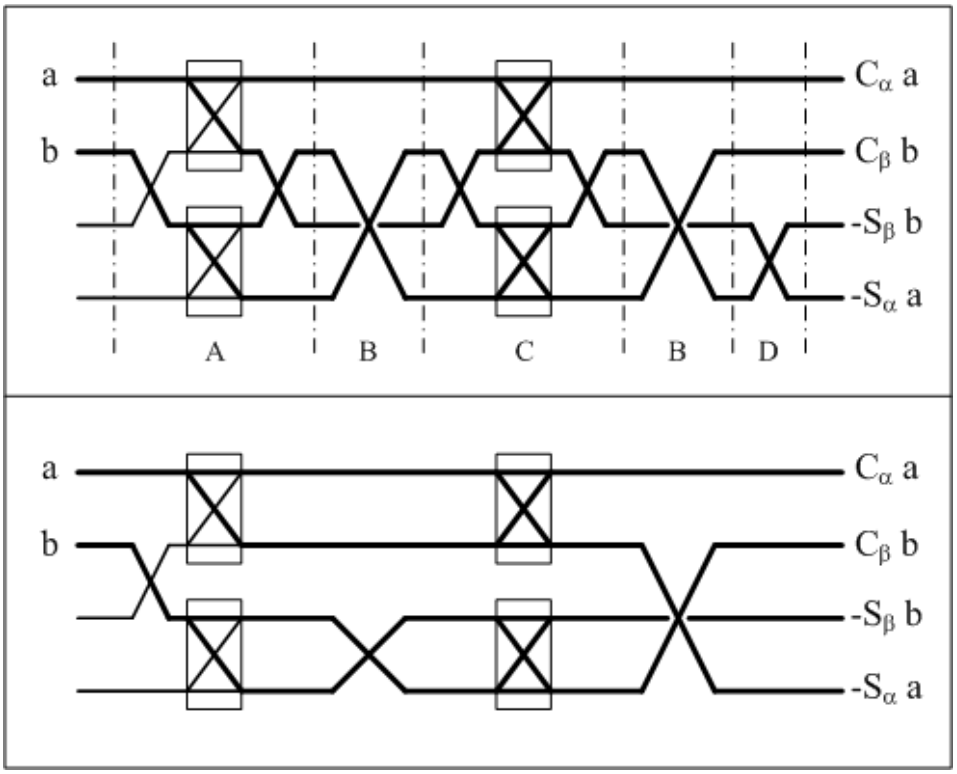

Figure 13: Diagram of states and equivalent simplified diagram of states representing the modified Griffiths-Niu copying machine.

Thus the diagrams of states are very useful in determining a quantum circuit of easier interpretation implementing the modified Griffiths-Niu copying machine, shown in figure 14.

To examine in more details the action of the Griffiths-Niu copying machine, it's worthwhile to observe what happens to the flow of information throughout the original circuit and to explicit the reduced density matrices of each intermediate state, according to the scheme in figure 15.

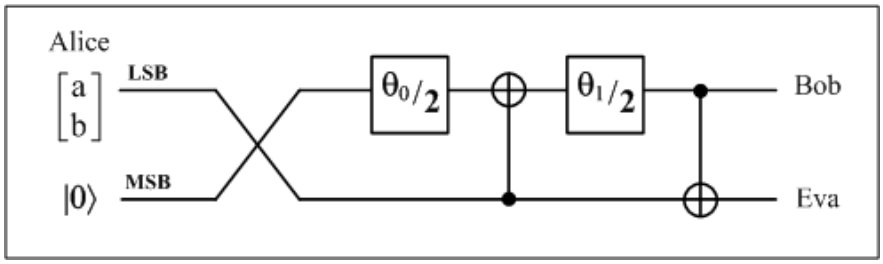

Figure 14: Quantum circuit equivalent to the circuit shown in figure 12 implementing the modified Griffith-Niu copying machine.

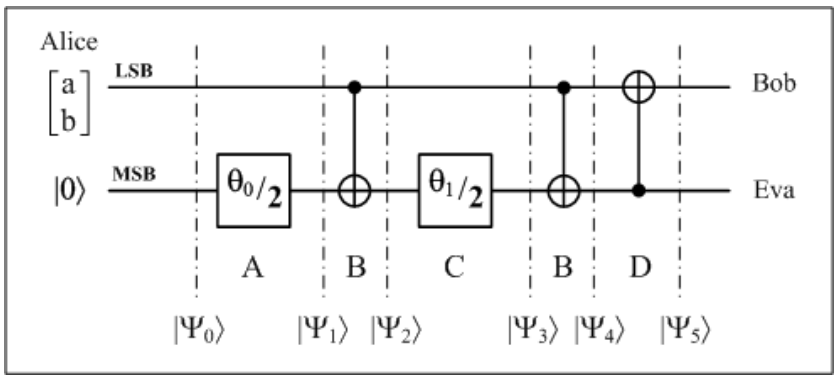

Figure 15: Intermediate states of quantum circuit implementing the modified Griffith-Niu copying machine.

Remembering the expressions for A, B, C, D operators given by equations 2 and 3, the intermediate states can be expressed by the following equations:

$$|\Psi_0\rangle = \begin{bmatrix} a \\ b \\ 0 \\ 0 \end{bmatrix} \tag{11}$$

$$|\Psi_1\rangle = A|\Psi_0\rangle = \begin{bmatrix} C_0\, a \\ C_0\, b \\ -S_0\, a \\ -S_0\, b \end{bmatrix} \tag{12}$$

$$|\Psi_2\rangle = B|\Psi_1\rangle = \begin{bmatrix} C_0\, a \\ -S_0\, b \\ -S_0\, a \\ C_0\, b \end{bmatrix} \tag{13}$$

$$|\Psi_3\rangle = C|\Psi_2\rangle = \begin{bmatrix} (C_0C_1 - S_0S_1)\, a \\ (C_0S_1 - S_0C_1)\, b \\ -(C_0S_1 + S_0C_1)\, a \\ (C_0C_1 + S_0S_1)\, b \end{bmatrix} \tag{14}$$

$$|\Psi_4\rangle = B|\Psi_3\rangle = \begin{bmatrix} (C_0C_1 - S_0S_1)\, a \\ (C_0C_1 + S_0S_1)\, b \\ -(C_0S_1 + S_0C_1)\, a \\ (C_0S_1 - S_0C_1)\, b \end{bmatrix} \tag{15}$$

$$|\Psi_5\rangle = D|\Psi_4\rangle = \begin{bmatrix} (C_0C_1 - S_0S_1)\, a \\ (C_0C_1 + S_0S_1)\, b \\ (C_0S_1 - S_0C_1)\, b \\ -(C_0S_1 + S_0C_1)\, a \end{bmatrix} = \begin{bmatrix} C_\alpha\, a \\ C_\beta\, b \\ -S_\beta\, b \\ -S_\alpha\, a \end{bmatrix} = |\Psi_{out}\rangle \tag{16}$$

In the following we will refer to least and most significant bits respectively with ^{B,E}. The reduced density matrices of the intermediate states are examined.

Matrix ρ_2

The state $|\Psi_1\rangle$ is not *entangled*, because the control-$\frac{\theta_0}{2}$ acts only on the most significant bit. So the first state for which it is useful to examine Bob and Eve's reduced density matrices is $|\Psi_2\rangle$:

$$\rho_2 = |\Psi_2\rangle\langle\Psi_2| \tag{17}$$

$$\rho_2^B = \begin{bmatrix} |a|^2 & -2\,C_0 S_0\,ab^* \\ -2\,C_0 S_0\,a^* b & |b|^2 \end{bmatrix} \tag{18}$$

$$\rho_2^E = \begin{bmatrix} C_0^2\,|a|^2 + S_0^2\,|b|^2 & -C_0 S_0 \\ -C_0 S_0 & S_0^2\,|a|^2 + C_0^2\,|b|^2 \end{bmatrix} \tag{19}$$

The upper equations show that the transformation of the density matrix ρ^B corresponds to a simple decoherence of the initial state, with fixed component Z:

$$\begin{cases} Z' = Z \\ X' = -2\,C_0 S_0\,X \\ Y' = -2\,C_0 S_0\,Y \end{cases} \tag{20}$$

The information of the amplitudes is then preserved, but not the coherences.

If $C_0^2 \neq S_0^2$, Eve can obtain part of the information on the amplitudes (the information is transferred on the most significant bit), but she does not possess any information on the coherences (the *c-not* gate cannot transmit them across the control qubit).

Matrix ρ_3

Bob and Eve's reduced density matrices corresponding to the intermediate state $|\Psi_3\rangle$ are examined by means of an analogous procedure:

$$\rho_3 = |\Psi_3\rangle\langle\Psi_3| \tag{21}$$

$$\rho_3^B = \begin{bmatrix} |a|^2 & -2\,C_0 S_0\,ab^* \\ -2\,C_0 S_0\,a^* b & |b|^2 \end{bmatrix} \tag{22}$$

Bob's information on amplitudes and coherences remains unchanged in respect to the previous intermediate state.

With some algebraic simplifications, Eve's reduced density matrix becomes:

$$\rho_3^E = \begin{bmatrix} C_\alpha^2\,|a|^2 + S_\beta^2\,|b|^2 & -(C_\alpha S_\alpha\,|a|^2 + C_\beta S_\beta\,|b|^2) \\ -(C_\alpha S_\alpha\,|a|^2 + C_\beta S_\beta\,|b|^2) & S_\alpha^2\,|a|^2 + C_\beta^2\,|b|^2 \end{bmatrix} \tag{23}$$

which shows that Eve gets some information on the Z component, but she does not possesses any information on the coherences yet.

Matrix ρ_4

Bob and Eve's reduced density matrices corresponding to the intermediate state $|\Psi_4\rangle$ are subsequently examined:

$$\rho_4 = |\Psi_4\rangle\langle\Psi_4| \tag{24}$$

$$\rho_4^B = \begin{bmatrix} |a|^2 & (C_1^2 - S_1^2)\, ab^* \\ (C_1^2 - S_1^2)\, a^*b & |b|^2 \end{bmatrix} \tag{25}$$

Bob's information on the amplitudes remains unchanged in respect to the previous intermediate states; the information on the coherences is reduced as shown.

With some algebraic simplifications, Eve's reduced density matrix becomes:

$$\rho_4^E = \begin{bmatrix} C_\alpha^2 |a|^2 + C_\beta^2 |b|^2 & -(C_\alpha S_\alpha |a|^2 + C_\beta S_\beta |b|^2) \\ -C_\alpha S_\alpha |a|^2 + C_\beta S_\beta |b|^2 & S_\alpha^2 |a|^2 + S_\beta^2 |b|^2 \end{bmatrix} \tag{26}$$

which shows that Eve has not yet got any information on the coherences.

Matrix ρ_5

Bob and Eve's reduced density matrices corresponding to the final state $|\Psi_5\rangle$ are finally examined:

$$\rho_5 = |\Psi_5\rangle\langle\Psi_5| \tag{27}$$

With some algebraic simplifications, Bob and Eve's reduced density matrices become respectively:

$$\rho_5^B = \begin{bmatrix} C_\alpha^2 |a|^2 + S_\beta^2 |b|^2 & C_\alpha C_\beta\, ab^* + S_\alpha S_\beta\, a^*b \\ C_\alpha C_\beta\, a^*b + S_\alpha S_\beta\, ab^* & S_\alpha^2 |a|^2 + C_\beta^2 |b|^2 \end{bmatrix} \tag{28}$$

$$\rho_5^E = \begin{bmatrix} C_\alpha^2 |a|^2 + C_\beta^2 |b|^2 & -(C_\alpha S_\beta\, ab^* + S_\alpha C_\beta\, a^*b) \\ -(C_\alpha S_\beta\, a^*b + S_\alpha C_\beta\, ab^*) & S_\alpha^2 |a|^2 + S_\beta^2 |b|^2 \end{bmatrix} \tag{29}$$

The two matrices correspond to the result of application of the modified Griffiths-Niu's copying machine. They cannot be drawn in any way from the previous matrices, ρ_4^B and ρ_4^E: the necessary information is then contained in the *entanglement* among the two qubits, especially for what concerning the coherences.

Finally, from the previous expressions it can be noticed that, although having the merit of great simplicity, this quantum copying machine presents the serious flaw of asymmetry and, above all, there is a displacement of the center of the Bloch sphere. These drawbacks are solved in the Bužek-Hillery quantum copying machine, to the price of a greater complexity.

3.2 The Bužek-Hillery's Copying Machine

The Bužek-Hillery quantum copying machine, [8],[9], is implemented by the quantum circuit shown in figure 16.

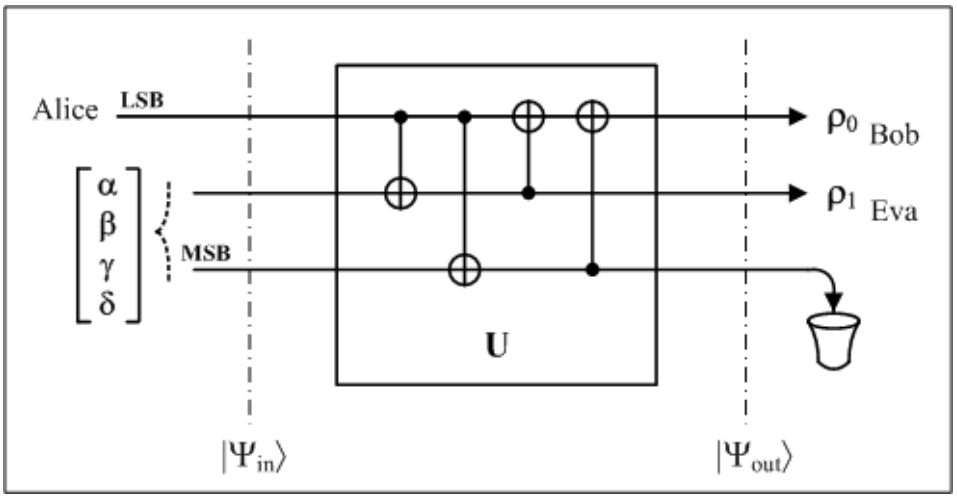

Figure 16: Quantum circuit implementing the Bužek-Hillery quantum copying machine.

The initial state of the ancillary qubits can be opportunely selected, according to the goal to ensue. Parameters can be considered assuming real values, with the condition of normalization holding:

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 1 \tag{30}$$

This quantum copying machine produces two distinct copies of an initial state. Thus it finds useful applications in quantum cryptography, in the situation when the state to copy is the one Alice is willing to send to Bob and Eve is instead intercepting: one copy will be used by Eve and the other one will be sent again to Bob, replacing the original state intercepted. We suppose that the quantum copying machine is totally controlled by Eve, so that she can opportunely vary the noise produced on the signal sent to Bob.[5]

[5]This is the most advantageous situation to eavesdropping and consequently the worst case from the point of view of the authorized communicating parties.

The great merit of this quantum copying machine consists in the fact that the matrix **U** produces only an exchange of states, while the control is entrusted entirely to the initial state of the ancillae. The mixing among the initial state, which the eavesdropper aims to copy, and the control state, in which the ancillary qubits are initialized, are very surprisingly given by simple tensor product of the corresponding states. Thus the action of the quantum copying machine consists in exchanging the states, as illustrated in the diagrams of states subsequently shown in figures 17 and 18.

In the analysis of the action of this quantum copying machine, the interesting point is the evaluation of the quality of the copy that remains to Eve, in comparison with the noise produced in the copy sent again to Bob; precisely, the relation occurring among these two factors will be examined for different assumptions on parameters of the state of the ancillary qubits introduced by Eve.

The four *c-not* gates produce the unitary matrix:

$$\mathbf{U} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{31}$$

Thus for the initial state:

$$|\Psi_{in}\rangle = \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} \otimes \begin{bmatrix} a \\ b \end{bmatrix} \tag{32}$$

the final state can be expressed by the following equation:

$$|\Psi_{out}\rangle = \mathbf{U}\,|\Psi_{in}\rangle = \mathbf{U} \begin{bmatrix} \alpha\,a \\ \alpha\,b \\ \beta\,a \\ \beta\,b \\ \gamma\,a \\ \gamma\,b \\ \delta\,a \\ \delta\,b \end{bmatrix} = \begin{bmatrix} \alpha\,a \\ \delta\,b \\ \gamma\,b \\ \beta\,a \\ \beta\,b \\ \gamma\,a \\ \delta\,a \\ \alpha\,b \end{bmatrix} \tag{33}$$

From this expression the density matrix and Bob and Eve's reduced density matrices can be immediately drawn: ρ_{Bob} by tracing over Eve's

qubit and the ancillary qubit and ρ_{Eve} by tracing over Bob's qubit and the ancillary qubit.

$$\rho_{Bob} = Tr_{Eve,anc}\{|\Psi_{out}\rangle\langle\Psi_{out}|\} = \tag{34}$$

$$= \begin{bmatrix} (\alpha^2+\delta^2)\,|a|^2 + (\beta^2+\gamma^2)\,|b|^2 & 2\,\alpha\delta\,ab^* + 2\,\beta\gamma\,a^*b \\ 2\,\alpha\delta\,a^*b + 2\,\beta\gamma\,ab^* & (\beta^2+\gamma^2)\,|a|^2 + (\alpha^2+\delta^2)\,|b|^2 \end{bmatrix}$$

$$\rho_{Eve} = Tr_{Bob,anc}\{|\Psi_{out}\rangle\langle\Psi_{out}|\} = \tag{35}$$

$$= \begin{bmatrix} (\alpha^2+\gamma^2)\,|a|^2 + (\beta^2+\delta^2)\,|b|^2 & 2\,\alpha\gamma\,ab^* + 2\,\beta\delta\,a^*b \\ 2\,\alpha\gamma\,a^*b + 2\,\beta\delta\,ab^* & (\beta^2+\delta^2)\,|a|^2 + (\alpha^2+\gamma^2)\,|b|^2 \end{bmatrix}$$

For the sake of completeness, the reduced density matrix of the ancillary qubit is also drawn, by tracing over Bob's qubit and Eve's qubit:

$$\rho_{anc} = Tr_{Bob,Eve}\{|\Psi_{out}\rangle\langle\Psi_{out}|\} = \tag{36}$$

$$= \begin{bmatrix} (\alpha^2+\beta^2)\,|a|^2 + (\gamma^2+\delta^2)\,|b|^2 & 2\,\alpha\beta\,ab^* + 2\,\gamma\delta\,a^*b \\ 2\,\alpha\beta\,a^*b + 2\,\gamma\delta\,ab^* & (\gamma^2+\delta^2)\,|a|^2 + (\alpha^2+\beta^2)\,|b|^2 \end{bmatrix}$$

These results provide the diagrams of states reported in figures 17 and 18.

The Symmetrical Case

Choosing $\beta = 0$, the superior coherence depends only from ab^* and not from a^*b (for the inferior coherence the situation is reversed). This is the first condition to assure the isotropy of the copies: the coefficients of the Bloch coordinates must be equal for both Bob and Eve, to preserve the symmetry of the Bloch sphere for each of the two states. If we call $\{X_i, Y_i, Z_i\}$, for $i = B, E$, the Bloch sphere coordinates associated to ρ_{Bob}, ρ_{Eve} after eavesdropping and $\{X, Y, Z\}$ the coordinates of the qubit sent from Alice to Bob before eavesdropping, as introduced in section 3.1, the condition of isotropy can be expressed by the relations:

$$X_i/X = Y_i/Y = Z_i/Z = S_i \qquad i = B, E$$

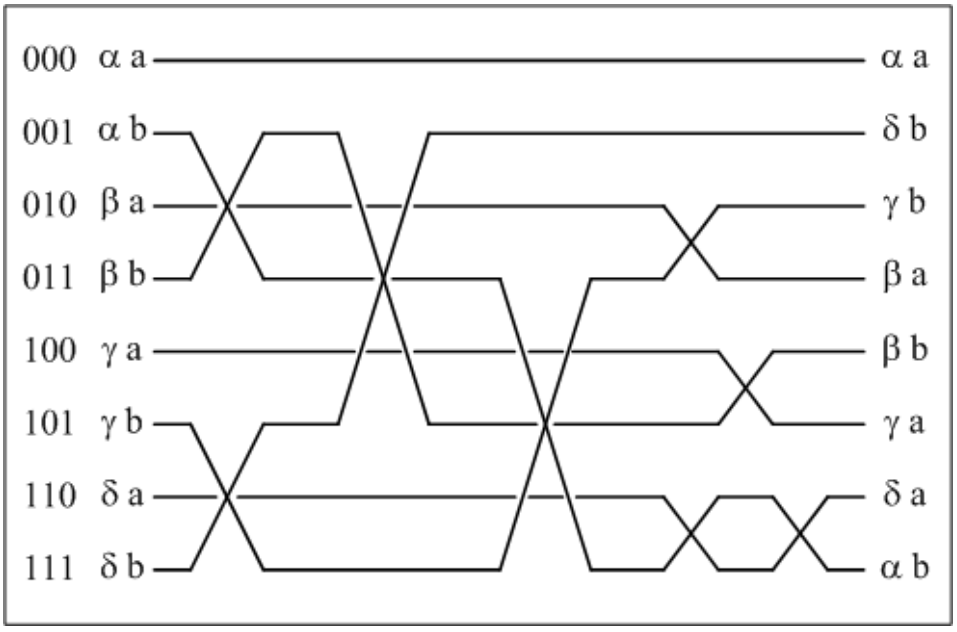

Figure 17: Diagram of states representing the Bužek-Hillery copying machine.

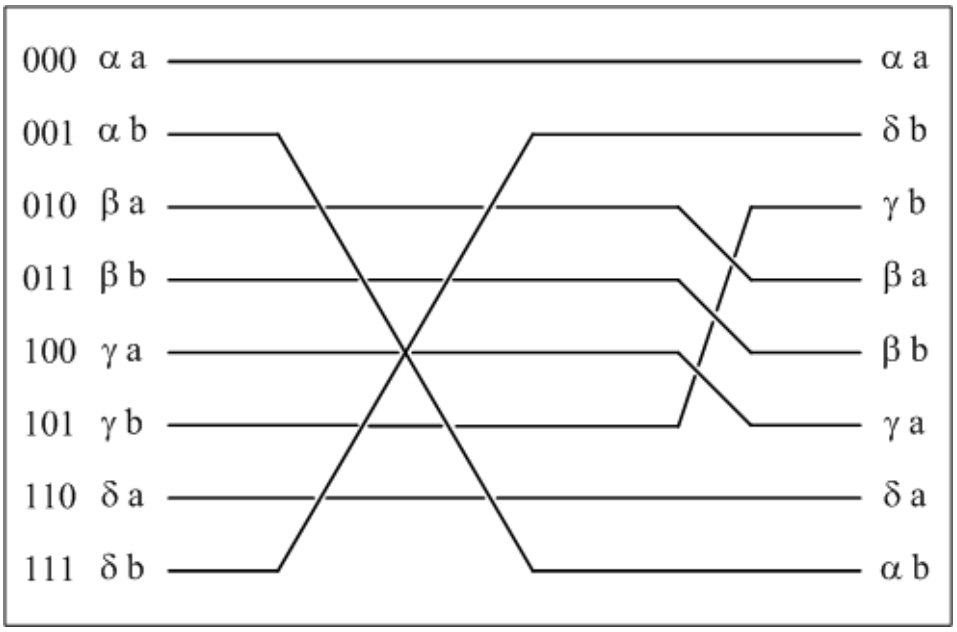

Figure 18: Simplified diagram of states representing the Bužek-Hillery copying machine.

The representation of Bob and Eve's density matrices, ρ_{Bob}, ρ_{Eve}, can be finally drawn, expressing the Bloch sphere coordinates $\{X_i, Y_i, Z_i\}$, for $i = B, E$, as a function of the coordinates $\{X, Y, Z\}$. Bob's coordinate transformation is given by:

$$\begin{cases} X_B = 2\,\alpha\delta\,X \\ Y_B = 2\,\alpha\delta\,Y \\ Z_B = (\alpha^2 + \delta^2 - \gamma^2)\,Z \end{cases} \tag{37}$$

Thus, to conserve the isotropy of the copies, besides imposing $\beta = 0$, it is necessary to add the condition:

$$\alpha^2 + \delta^2 - \gamma^2 = 2\,\alpha\delta \tag{38}$$

always considering the condition of normalization:

$$\alpha^2 + \gamma^2 + \delta^2 = 1 \tag{39}$$

Eve's coordinate transformation is given by:

$$\begin{cases} X_E = 2\,\alpha\gamma\,X \\ Y_E = 2\,\alpha\gamma\,Y \\ Z_E = (\alpha^2 + \gamma^2 - \delta^2)\,Z \end{cases} \tag{40}$$

and the condition of isotropy:

$$\alpha^2 + \gamma^2 - \delta^2 = 2\,\alpha\gamma \tag{41}$$

Let us consider α as a free parameter; it's worthwhile to express the solution of the previous isotropy conditions in respect to α:

$$\beta = 0 \qquad \gamma = \frac{\alpha}{2} - \sqrt{\frac{1}{2} - \frac{3}{4}\alpha^2} \qquad \delta = \frac{\alpha}{2} + \sqrt{\frac{1}{2} - \frac{3}{4}\alpha^2} \tag{42}$$

Equations (37) and (40) become:

$$\begin{cases} X_B = 2\,\alpha\delta\,X = S_B\,X \\ Y_B = 2\,\alpha\delta\,Y = S_B\,Y \\ Z_B = 2\,\alpha\delta\,Z = S_B\,Z \end{cases} \tag{43}$$

$$\begin{cases} X_E = 2\,\alpha\gamma\,X = S_E\,X \\ Y_E = 2\,\alpha\gamma\,Y = S_E\,Y \\ Z_E = 2\,\alpha\gamma\,Z = S_E\,Z \end{cases} \tag{44}$$

with:

$$\frac{1}{\sqrt{2}} \leq \alpha \leq \sqrt{\frac{2}{3}} \tag{45}$$

where the left limitation is obtained by imposing S_B and S_E non negative and the right limitation is obtained from the reality condition for the square root in equation (42).

This detailed analysis provide the plots in figures 19 and 20, that clearly illustrates the relation between Eve's intrusion and the quality of the state received by Bob.

Figure 19 shows the behavior of the coefficients $\{S_B, S_E\}$, which quantify the deformation of Bob and Eve's states respectively, as shown explicitly in equations (43) and (44), as a function of the free parameter α. For $\alpha = \frac{1}{\sqrt{2}}$, Eve draws no information from her own copy, while Bob receives the state without errors (his copy coincides with the state originally sent by Alice). For $\alpha = \sqrt{\frac{2}{3}}$, Eve and Bob obtain the same states, corresponding to:

$$S_B = S_E = \frac{2}{3}$$

and the plot shows also all intermediate situations. Notice that Eve's gain of information is tightly correlated to presence of errors in the state received by Bob.

Figure 20 show the behavior of the coefficient S_B, which quantifies the deformation of Bob's state, as a function of the coefficient S_E, which quantifies the deformation of Eve's state, both as a function of the free parameter α. Once again, Eve's gain of information is tightly correlated to presence of errors in the state received by Bob.

The Asymmetrical Case

In the previous section, the equality of coefficients of all the Bloch sphere coordinates was required to assure total symmetry of the quantum copies.

Yet such conditions are really necessary only for a *six-state* protocol, that is to say a protocol in which Alice and Bob can decide arbitrarily to measure along all of the three axes X, Y, Z. The isotropy conditions may be relaxed for a *four-state* protocol, which allows Alice and Bob to use two different bases of measurement, equivalently to measure along two of the three axes of the Bloch sphere.

Let us consider the case when Eve knows that Alice and Bob use a four-state protocol and that she also knows the choice of the two possible bases of measurement; therefore it is not necessary for Eve to reproduce as correctly as possible the coordinates X, Y, Z, but she needs only to faithfully reproduce the two coordinates involved in the protocol. Thus it is not necessary

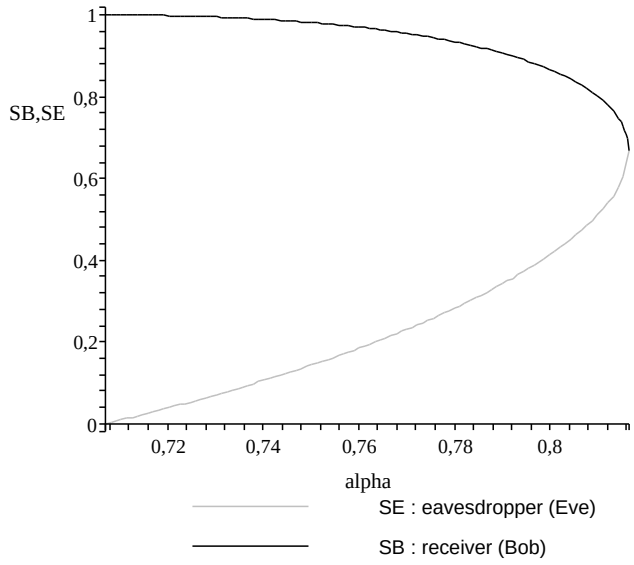

Figure 19: S_B, S_E plot as a function of the free parameter α in the symmetrical case.

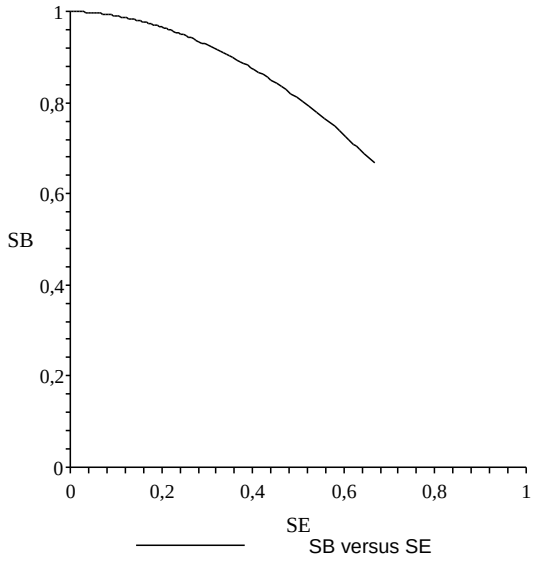

Figure 20: Plot of the coefficient S_B as a function of the coefficient S_E.

to impose the condition of symmetry for all the three coordinates, but such condition has to be applied only at the two coordinates considered in the protocol.

So it's worthwhile to verify if the choice of an asymmetrical protocol may offer advantageous conditions to Eve, now that a faithful reproduction of states on each coordinate is no longer needed. The choice of the coordinate not to be considered for imposition of symmetry influences significantly the difficulty of the analysis of the asymmetrical case. In accordance with literature, the maximal simplicity of analysis results for a symmetrical cloning in the coordinates X, Y and neglecting the coordinate Z, that means considering equatorial states.

Equatorial case

The neglect of the coordinate Z and the imposition of the condition $\beta = 0$ lead to the Bloch sphere coordinate tranformations:

$$\begin{cases} X_B = 2\,\alpha\delta\,X \\ Y_B = 2\,\alpha\delta\,Y \end{cases} \qquad S_B = 2\,\alpha\delta \tag{46}$$

$$\begin{cases} X_E = 2\,\alpha\gamma\,X \\ Y_E = 2\,\alpha\gamma\,Y \end{cases} \qquad S_E = 2\,\alpha\gamma \tag{47}$$

with the condition of normalization:

$$\alpha^2 + \gamma^2 + \delta^2 = 1 \tag{48}$$

By replacing the expressions for S_B and S_E, the condition of normalization (48) becomes:

$$S_B^2 + S_E^2 = -4(\alpha^4 - \alpha^2) \tag{49}$$

Following the procedure in ref.[10] we maximize S_B, for fixed values of S_E, varying the free parameter α, and this procedure leads to the results:

$$\alpha = \frac{1}{\sqrt{2}} \qquad S_B^2 + S_E^2 = 1 \tag{50}$$

Thus the optimum parameters are given by the following values:

$$\begin{cases} \alpha = \frac{1}{\sqrt{2}} \\ \beta = 0 \\ \gamma = \frac{1}{\sqrt{2}}\,S_E \\ \delta = \frac{1}{\sqrt{2}}\,S_B = \sqrt{\frac{1}{2} - \gamma^2} \end{cases} \tag{51}$$

4 Conclusions and Directions for Future Research

With the present work we desired to present a much more detailed analysis of quantum circuits in comparison with what can be currently found in literature, by introducing a new graphic representation of quantum states and of information's flow in quantum algorithms. We also aimed at illustrating this new representation by diagrams of states with concrete examples: to this purpose we chose to explore two models of quantum copying machines in cryptographic protocols.

Quantum algorithms can currently be listed under a few main classes and this suggest that the state of the art in quantum information theory is still far from a complete understanding and full exploitation of the potentialities offered by Quantum Mechanics for computation and information processing. In our opinion, this might be due both to the fact that quantum computation is a rather new discipline in respect to conventional computation and to the necessity, for a quantum algorithm whose importance may be significant, to overcome in performances the classical counterparts.

Thus the aim of the graphic representation of states is to promote the creation of a "quantum insight" that should be useful for an easier comprehension of quantum circuits and consequently of quantum algorithms derived from them. Moreover, when creating new algorithms, also the procedure of finding suitable quantum circuits would be easier with the aid of a graphic visualization of the desired transformation for the quantum states of the systems considered.

The method, used here for the study of quantum copying machines, has indeed shown itself to be extremely successful for the representation of the involved quantum operations and it has allowed to point out the characteristic aspects of quantum computation; [13].

5 Appendix

5.1 Synthesis of the Control State

The present appendix offers a possible procedure to generate the control state $|\Psi\rangle = \{\alpha|00\rangle + \beta|01\rangle + \gamma|01\rangle + \delta|11\rangle\}$ for the Bužek-Hillery copying machine, introduced in section 3.2. The state $|\Psi\rangle$ can be obtained with three parameters $\theta_1, \theta_2, \theta_3$, as expressed by the following equation:

$$|\Psi\rangle = \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} \cos\theta_1 \cos\theta_2 \\ \cos\theta_1 \sin\theta_2 \\ \sin\theta_1 \cos\theta_3 \\ \sin\theta_1 \sin\theta_3 \end{bmatrix} \tag{52}$$

and it can thus be generated by the quantum circuits in figure 21. Defining:

$$C_i = cos\,\theta_i \qquad S_i = sin\,\theta_i \qquad i = 1, 2, 3 \tag{53}$$

the following operators are respectively associated to these circuits:

$$U_1 = \begin{bmatrix} C_1 & 0 & -S_1 & 0 \\ 0 & C_1 & 0 & -S_1 \\ S_1 & 0 & C_1 & 0 \\ 0 & S_1 & 0 & C_1 \end{bmatrix} \qquad U_2 = \begin{bmatrix} C_2 & -S_2 & 0 & 0 \\ S_2 & C_2 & 0 & 0 \\ 0 & 0 & C_3 & -S_3 \\ 0 & 0 & S_3 & C_3 \end{bmatrix} \tag{54}$$

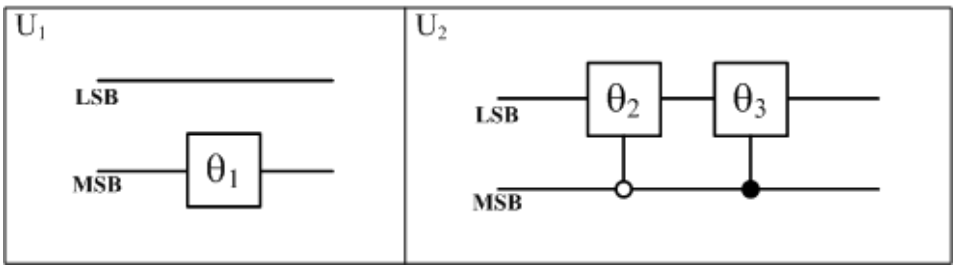

Figure 21: Quantum circuits implementing the synthesis of the control state.

Applying the matrices U_1, U_2 to the initial state $|00\rangle$, the final state can be expressed by the following equation:

$$U_2 U_1 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} C_2\,C_1 \\ S_2\,C_1 \\ C_3\,S_1 \\ S_3\,S_1 \end{bmatrix} \tag{55}$$

Observe that, imposing the condition $\beta = 0$, and so considering the symmetrical case, the *controlled-*θ_2 gate is absent.

The diagram of states for the synthesis of the control state $|\Psi\rangle$ is shown in figure 22 and clearly illustrates the information's flow that generates the desired state.

The initial state is the state $|00\rangle$ and the corresponding line in the diagram is marked. As usual, thin lines represent absence of information. The diagram evidently shows the information's flow that produces the control parameters $\{\alpha, \beta, \gamma, \delta\}$ and how the system is characterized by three total degrees of freedom, given by the three parameters $\theta_1, \theta_2, \theta_3$. Observe that the gate θ_1 does not produce *entanglement* (unlike the gates θ_2 and θ_3) since it does not act only on a partition of the four states, as explained in section 2.1.1.

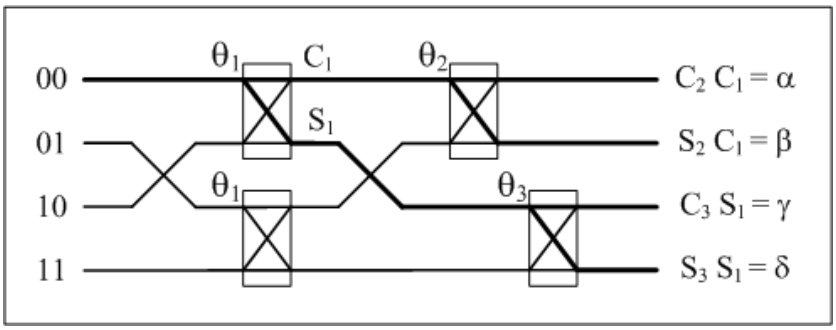

Figure 22: Diagram of the states representing the synthesis of the control state.

5.2 Relation between the *Fidelity* and the Parameter S of the Quantum Copying Machines

Let us define the *fidelity*:

$$\mathcal{F} = |\,\langle\Psi|\,\rho\,|\Psi\rangle\,| = \tag{56}$$

$$= \text{probability that the obtained state would successfully pass a test for being in the original state.}$$

Due to symmetry, the relation between the *fidelity* and the parameter S of the quantum copying machines can be expressed as follows, considering the state $|0\rangle$ for both Bob and Eve:

$$\begin{aligned} \mathcal{F} &= \left| \begin{bmatrix} 1 & 0 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1+Z_{B,E} & X_{B,E}-i\,Y_{B,E} \\ X_{B,E}+i\,Y_{B,E} & 1-Z_{B,E} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right| \\ &= \frac{1}{2}\,(1+Z_{B,E}) = \frac{1}{2}\,(1+S_{B,E}) \end{aligned} \tag{57}$$

Acknowledgements

The authors gratefully thank the anonymous referees, whose comments and suggestions have helped us to greatly improve a previous version of this paper.

References

[1] G. Benenti, G. Casati, G. Strini: *Principles of Quantum Computation and Information, Volume I: Basic Concepts*, World Scientific, 2004

[2] G. Benenti, G. Casati, G. Strini: *Principles of Quantum Computation and Information, Volume II: Basic Tools And Special Topics*, World Scientific, 2006

[3] M.A. Nielsen, I.L. Chuang: *Quantum Computation and Quantum Information*, Cambridge University Press, 2000

[4] D. Dieks: *Communication by EPR devices*, Phys. Lett. A 92, 271 (1982)

[5] W.K. Wootters and W.H. Zurek: *A Single Quantum Cannot Be Cloned*, Nature 299, 802 (1982)

[6] C.S. Niu and R.B. Griffiths: *Optimal Copying of One Quantum Bit*, Phys. Rev. A 58 (1998) 4377-4393

[7] C.S. Niu and R.B. Griffiths: *Two Qubit Copying Machine for Economical Quantum Eavesdropping*, Phys. Rev. A 60 (1999) 2764-2776

[8] V. Bužek and M. Hillery: *Quantum Copying: Beyond the No-Cloning Theorem*, Phys. Rev. A 54, 1844 (1996)

[9] V. Bužek and M. Hillery: *Universal Optimal Cloning of Qubits and Quantum Registers*, quant-ph/9801009

[10] A.T. Rezakhani, S. Siadatnejad, A.H. Ghaderi: *Separability in Asymmetric-Phase Covariant Cloning*, quant-ph/0312024

[11] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, A. Sanpera: *Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels*, The American Physical Society, 1996

[12] S. Felloni, G. Strini (supervisor), M. Galuzzi, S. Kasangian (cosupervisors): *Problemi di Purificazione dell'Entanglement in Crittografia Quantistica*, Master Thesis: Dipartimento di Matematica Federigo Enriques, Università degli Studi di Milano, via Saldini 50, Milano, a.y. 2004/2005

[13] This initial formulation of the graphic representation of states will be followed by application of the method to more complex and meaningful cases, which are going to be explored in future works: S. Felloni et al., paper in preparation.

For further references see [1], [2].